Criado por:	Assunto	Versão	Data	Cod
Bruno Ricardo Pin	Auditoria de Processos e Sistemas Informatizados	1	04/01/2024	MI120

Objetivo da Auditoria:

Garantir a conformidade e a eficácia das práticas de gestão de senhas, identificando possíveis vulnerabilidades e garantindo a segurança dos sistemas.

- Identificar vulnerabilidades de segurança.
- Garantir conformidade com políticas de segurança e regulamentações.
- Avaliar a eficiência operacional e a integridade dos sistemas.
- Verificar atualizações de software e patches.

Procedimentos de Auditoria de senha:

1. **Revisão das Políticas e Procedimentos de Senhas:**

   Verificar se as políticas de senha estão atualizadas e alinhadas com as melhores práticas de segurança.

   Assegurar que as políticas incluam requisitos mínimos de complexidade de senha, atualização periódica, restrições de reutilização e outras diretrizes relevantes.

2. **Avaliação da Implementação das Políticas:**

   Verificar se as políticas de senha são aplicadas em todos os sistemas e plataformas relevantes.

   Analisar se as políticas estão sendo seguidas por meio de revisão de registros de alterações de senha e logs de acesso.

3. **Análise da Segurança das Senhas:**

   Verificar se as senhas seguem boas práticas de segurança (complexidade, comprimento, falta de padrões previsíveis).

   Avaliar a força das senhas armazenadas, se estão adequadamente protegidas e criptografadas.

4. **Revisão de Acesso e Controle:**

   Analisar os níveis de acesso concedidos a diferentes usuários.

   Garantir que a autenticação de múltiplos fatores seja implementada quando apropriado.

5. **Revisão de Incidentes Recentes:**

   Investigar incidentes de segurança recentes relacionados a senhas para identificar áreas de melhoria.

Procedimentos de Auditoria de acesso:

1. **Revisão de Controles de Acesso:**

   Verificar a adequação dos controles de acesso aos sistemas e dados sensíveis.

   Revisar permissões de usuário e níveis de acesso para garantir que estejam alinhados com as funções e responsabilidades.

2. **Análise de Logs e Registros de Auditoria:**

   Revisar registros de acesso, logs de eventos e atividades do sistema para identificar padrões ou atividades suspeitas.

   Verificar se existem lacunas na geração ou retenção de logs.

3. **Avaliação de Políticas de Segurança e Auditoria:**

   Verificar se as políticas e procedimentos de segurança de TI estão de acordo com as melhores práticas e regulamentações relevantes.

   Assegurar que auditorias internas e externas estejam sendo realizadas regularmente.

4. **Verificação de Segurança Física e Lógica:**

   Avaliar a segurança física dos dispositivos e servidores que armazenam dados sensíveis.

   Garantir que as medidas de segurança lógica, como firewalls, antivírus e criptografia, estejam implementadas e atualizadas.

5. **Revisão de Incidentes de Segurança:**

   Analisar incidentes anteriores para identificar pontos fracos ou vulnerabilidades que possam ter permitido acessos indevidos ou adulterações.

Auditoria de servidores, estações de trabalho, laptops:

1. **Verificação de Segurança:**

   Avaliação de vulnerabilidades.

   Verificação de configurações de antivírus, e regras GPO.

   Análise de registros de segurança (logs).

1. **Conformidade e Atualizações:**

   Verificar conformidade com políticas de segurança e regulamentos.

   Revisar atualizações de software e patches.

   Avaliar a eficácia das medidas de segurança implementadas.

2. **Inventário e Gerenciamento:**

   Criar ou atualizar inventário de hardware e software.

   Verificar a conformidade com políticas de licenciamento.

   Avaliar o gerenciamento de ativos e seu ciclo de vida.

Auditoria para verificar adulterações e acessos indevidos

1. **Escopo da Auditoria:**

   Identificar os sistemas críticos e sensíveis que necessitam de verificação.

   Incluir servidores, laptops e computadores com dados sensíveis ou de alta importância.

2. **Avaliação de Integridade e Autenticidade:**

   Verificar a integridade dos arquivos críticos nos sistemas.

   Examinar logs de alterações de arquivos e diretórios para identificar mudanças não autorizadas.

3. **Controle de Acessos:**

   Revisar os logs de acesso para identificar acessos não autorizados.

Verificar permissões de usuário e grupos em arquivos e diretórios sensíveis.

Analisar logs de autenticação para identificar tentativas de acesso indevidas.

4. **Monitoramento de Segurança:**

   Analisar registros de segurança (logs) para detectar padrões incomuns ou suspeitos.

   Utilizar ferramentas de detecção de intrusão para identificar atividades anômalas.

5. **Análise de Vulnerabilidades:**

   Realizar varreduras de vulnerabilidades nos sistemas para identificar pontos fracos.

   Avaliar os sistemas em relação a patches e atualizações de segurança ausentes.

6. **Revisão de Configurações de Segurança:**

   Verificar configurações de firewall, antivírus, e outras ferramentas de segurança.

   Avaliar políticas de senha e de acesso para garantir que sejam adequadas e aplicadas corretamente.

Auditorias Periódicas de intrusão de rede;

1. **Escopo da Auditoria:**

   Identificar todos os firewalls e soluções antivírus em uso na infraestrutura.

   Incluir tanto hardware quanto software relacionado à proteção de perímetro.

2. **Políticas e Configurações:**

   Revisar e documentar as políticas de firewall em vigor, incluindo regras de filtragem de tráfego, políticas de acesso, etc.

   Verificar se as configurações do firewall estão alinhadas com as melhores práticas de segurança.

3. **Regras de Firewall:**

   Analisar as regras de firewall existentes para identificar possíveis brechas de segurança ou regras desnecessárias.

   Verificar a lógica por trás das regras para garantir a eficácia e relevância delas.

4. **Logs e Monitoramento:**

   Verificar se os logs de firewall e antivírus estão sendo devidamente registrados e monitorados.

   Analisar os registros para identificar padrões de tráfego suspeitos ou atividades maliciosas.

5. **Atualizações e Patches:**

   Revisar a política de atualizações e patches para o firewall e antivírus.

   Garantir que todos os dispositivos estejam atualizados com as últimas correções de segurança.

6. **Desempenho e Eficácia:**

   Avaliar o desempenho do firewall e antivírus em termos de detecção de ameaças e tempo de resposta.

   Verificar se as soluções implementadas estão protegendo a rede de maneira eficaz.

7. **Conformidade e Regulamentações:**

   Verificar se as políticas de firewall e antivírus estão em conformidade com regulamentações pertinentes ao setor.

Auditoria de WhatsApp:

1. Ferramentas Utilizadas:

Analisar se o backup está ocorrendo, verificando se conversas antigas estão armazenadas.

2. Análise das Conversas:

Revise as conversas relevantes, de departamentos com alto risco de vazamento de dados pessoais.

Identificar informações ou comportamentos pertinentes à investigação ou à conformidade.

3. Segurança e Privacidade:

Assegure-se de que todas as informações sensíveis sejam tratadas com cuidado, seguindo políticas de segurança e privacidade.

Validar a senha e realizar a troca de tempos em tempos (Período sugerido 90 dias)